UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/822,226	04/08/2004	Sumeet Singh	15670-075001/ SD2004-151	1313

20985 7590 02/04/2009		
FISH & RICHARDSON, PC	EXAMINER	
P.O. BOX 1022	OKORONKWO, CHINWENDU C	
MINNEAPOLIS, MN 55440-1022		

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
02/04/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

	Application No.	Applicant(s)
Office Action Summary	10/822,226	SINGH ET AL.
	Examiner	Art Unit
	CHINWENDU C. OKORONKWO	2436

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *10 November 2008*.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-35,69-79,88 and 89* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-35, 69-79,88 and 89* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
      application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1.   In response to communications filed on 11/10/2008, the Examiner acknowledges

the amendments made to the claims and have both considered and applied them to the

claims.

Claims 1-35, 69-79, 88 and 89 are presented for examination.

Response to Remarks/Arguments

2.   Applicant's arguments with respect to the rejection of the claims have been fully

considered but they are not persuasive. However to make the record clear, the previous

action has been modified to clearly address the applicant's invention. Therefore, this is

a non final action based on a new ground of rejection.

2.1   In response to Applicant argument that the Teal reference does not teach or

suggest a collection of data items that is to be analyzed to identify a network attack be

reduced to a reduced data collection / portions of the data on a network are to be

obtained and data reduced, the Examiner respectfully disagrees citing column 4 lines 5-

46 which recites in part "data collector converters 14 collect the network data and

convert the network data into predetermined formats for analysis." The disclosure here

of a data collector which converts the network data into predetermined formats for

analysis reads upon the argued reduced data collection, as this "predetermined format"

is an alteration of the original data collected as opposed to analyzing the entire original

data as collected, before the conversion.

2.2   In response to the Applicant argument that the Teal reference does not teach or

suggest a plurality of reduced data items being analyzed to detect common elements /

such reduced data portions be analyzed to find network content which repeats a

specified number of times in order to establish said network content as frequent content,

the Examiner respectfully disagrees citing column 4 lines 5-46 which recites in part

"Intrusion detection analysis engine 16 analyzes network data to look for specific

patterns that indicate malicious activity on the network." The disclosure here of a

intrusion detection analysis engine which analyzes the converted data for "specific

patterns" reads upon the argued reduced data items being analyzed to detect common

elements, as this data that has been converted to a predetermined format is now

analyzed for specific patterns (elements).

2.3   In response to the Applicant argument that the Adjaoute reference does not

teach or suggest the "sub models [which] obtain portions of the data on a network data

reduces them, as recited in claim 69" or "sub models [which] analyzes such reduced

data portions to find network content which repeats a specified number of times in order

to establish said network content as frequent content, as recited in claim 69" the

Examiner respectfully reminds the Applicant of the 102(e) and 103(a) rejections

provided in the Office Action being responded to (dated 08/11/2008), thus a portion of

the rejection is cared for by the first reference of record, Teal, and the remaining portion

is disclosed by the secondary reference, Adjaoute. Further, the Examiner notes that

each argument of the Applicant in this response has been addressed, although some

arguments were repeated as some claim limitations as very similar.

Applicant has not overcome the rejection.

Claim Rejections - 35 USC § 103

1.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

        Claims 1-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over _Teal_

(US Patent No. 6,477,651 B1 _hereinafter_ Teal) in view of Hrabik et al (US Patent No.

6,988,208 B2 _hereinafter_ Hrabik).

        Regarding claim 1, Teal, discloses a machine implemented method for

automatically identifying common content to use in identifying an intrusive

network attack comprising: obtaining a collection of data (4:23-25 – "data

collected") to be analyzed to identify the network attack (4:5-46 – "data collector

converter 14 is used for each type of network data collected from the network"); a

constant predetermined relation with data items in the data collection (4:16-27 –

"predetermined formats"); analyzing a plurality of said reduced data items to

detect common elements (4:33-34 – "network data to look for specific patterns "),

said analyzing identifying common content indicative of a network attack (4:5-46

– "data collector converters 14 collect the network data and convert the network

data into predetermined formats for analysis" and "Intrusion detection analysis

engine 16 analyzes network data to look for specific patterns that indicate

malicious activity on the network").

Teal is silent in disclosing reducing said data items in said collection to reduce

said data collection to a reduced data collection of reduced data items, wherein

the reduced data items in the reduced data collection have a smaller size and at

least some of the data items in the data collection that differ are reduced to the

same reduced data item, however Hrabik does provide such a disclosure (9:48-

56 – "a collection engine 502 collect[s] the event-data from various devices on

the target network" and 10:24-41 – "classification process is accomplished by a

classification engine 506. Once the log analyzer/event consolidator engine has

uncovered the source of the event message, the system proceeds to classify the

event by determining the overall meaning of the message and specific details

necessary to make an evaluation of the significance of the event ... classification

engine will combine these similar messages from different sources, reducing the

level of redundancy within the data").

It would have been obvious for one of ordinary skill in the art, at the time of the
invention, to have been motivated to combine the disclosures of Teal with Hrabik
as both are directed towards protecting computer systems/networks from security
breaches. Hrabik provides motivation for the combination in the recitation, "a
fundamental weakness shared in common by current intrusion detection and
response systems is their 'flat' or non-hierarchical implementation" (1:50-53) and
further "after the events have been consolidated and classified, they enter the
correlation stage ... performed by a hierarchy of event analyzers ... to reduce the
number of security events, each event analyzer combines related security events
into a single security ticket. Event analyzers can also use the results of
vulnerability scans ... to prioritize detected security events" (10:62-67 and 11:1-
20). Thus the combination here provides an obvious disclosure of the reduction
of collected data for the benefit of allowing for more efficient analyzing of data.

Regarding claim 2, Teal, discloses a method wherein said analyzing comprises
determining frequently occurring sections of message information (4:5-46 –
"Intrusion detection analysis engine 16 analyzes network data to look for specific
patterns that indicate malicious activity on the network. These patterns, known as
signatures, are generally unique to each type of vulnerability of network.")

Regarding claim 3, Teal, discloses a method wherein said analyzing comprises
determining that increasing number of sources and destinations that are sending
and/or receiving data (4:19-27 – "Data source 12 can include network routers
and servers that provide network traffic data, audit trail data, system information
data, and other data sources. In one embodiment, a data collector converter 14
is used for each type of network data collected from the network.")

Regarding claim 4, Teal, discloses a method further comprising analyzing for the
presence of a specified type of code within said collection of data (col. 1 lines 60-
67 – "analyzing an incoming data packet from the public network. The incoming
data packet is then matched against known forms of attack on the private
network.").

Claims 5-35, 69-79 and 88-89 are rejected under 35 U.S.C. 103(a) as being
unpatentable over Teal (US Patent No. 6,477,651 B1) in view of Hrabik et al (US Patent
No. 6,988,208 B2 *hereinafter* Hrabik) and further in view of Adjaoute (US Patent No.
7,089,592 B2).

Regarding claim 5, Teal and Hrabik, are silent in disclosing after said analyzing
determines said frequently occurring sections of message information, carrying

out an additional test on said frequently occurring sections of message

information, however, <u>Adjaoute</u> does provide such a disclosure (11:19-31 –

"model component 54 is a program that takes data associated with an electronic

transaction and decides whether the transaction is fraudulent … [it] also takes

data associated with network usage and decides whether there is network

intrusion … [and] consists of an extensible collection of integrated sub-models

55, each of which contributes to the final decision").

It would have been obvious for one of ordinary skill in the art, at the time of

the invention to have been motivated to combine the inventions of Teal

and Adjaoute because both inventions are directed towards intrusion

detection systems which analyze network data in determining risks. The

motivation and benefit for the combination/modification of Teal and Hrabik

is provided by Adjaoute, which recites, "[it is] desirable to provide systems

and methods for dynamic detection and prevention of electronic fraud and

network intrusion that are able to detect and prevent fraud and network

intrusion across multiple networks and industries … [and] that employ an

integrated set of intelligent technologies."

Regarding <u>claim 6</u>, <u>Teal</u>, discloses a method wherein said carrying out the

additional test comprises looking for an increasing number of at least one of

sources and destinations of said frequently occurring sections of message

information (4:19-27 – "Data source 12 can include network routers and servers that provide network traffic data, audit trail data, system information data, and other data sources. In one embodiment, a data collector converter 14 is used for each type of network data collected from the network.").

Regarding claim 7, Teal, discloses a method wherein said carrying out the additional test comprises looking for code or opcode (operation code) within the frequently occurring sections (4:33-39 – "intrusion detection analysis engine 16 analyzes network data to look for specific patterns that indicate malicious activity on the network").

Regarding claim 8, Teal, discloses a method wherein said reducing said data items comprises carrying out a hash function on said data items (4:33-39 – "These patterns, known as signatures, are generally unique to each type of vulnerability of the network.").

Regarding claims 9, Teal, is silent in disclosing a method wherein said determining frequently occurring sections comprises using at least first, second and third data reduction techniques on each said data item, to obtain at least first, second and third reduced data items, counting said first, second and third reduced data items and establishing said frequently occurring sections when all of said at least first second and third reduced data items have a frequency of

occurrence greater than a specified amount, however , <u>Adjaoute</u> does provide

such a disclosure (11:19-31 – "model component 54 is a program that takes data

associated with an electronic transaction and decides whether the transaction is

fraudulent … [it] also takes data associated with network usage and decides

whether there is network intrusion … [and] consists of an extensible collection of

integrated sub-models 55, each of which contributes to the final decision").

It would have been obvious for one of ordinary skill in the art, at the

time of the invention to have been motivated to combine the inventions of

Teal and Adjaoute because both inventions are directed towards intrusion

detection systems which analyze network data in determining risks. The

motivation and benefit for the combination/modification of Teal is provided

by Adjaoute, which recites, "[it is] desirable to provide systems and

methods for dynamic detection and prevention of electronic fraud and

network intrusion that are able to detect and prevent fraud and network

intusion acreoss multiple networks and industries … [and] that employ an

integrated set of intelligent technologies."

Regarding <u>claim 10</u>, <u>Teal</u>, discloses a collection of data items comprises a

portion of the network payload (4:16-27).

Regarding claim 11, Teal, is silent in disclosing a method wherein said carrying

out the additional test comprises: maintaining a first list of unassigned addresses;

forming a second list of sources that have sent to addresses on said first list; and

comparing a current source of a frequently occurring section to said second list,

however Hrabik does provide such a disclosure (11:50-54 – "Smart actions of the

provided security system are issued by event analyzers and can counteract a

threatening security event, for example, by increasing the level of detail recorded

on specific actions, IP addresses or users").

It would have been obvious for one of ordinary skill in the art, at the time of the

invention, to have been motivated to combine the disclosures of Teal with Hrabik

as both are directed towards protecting computer systems/networks from security

breaches. Hrabik provides motivation for the combination in the recitation, "a

fundamental weakness shared in common by current intrusion detection and

response systems is their 'flat' or non-hierarchical implementation" (1:50-53) and

further "after the events have been consolidated and classified, they enter the

correlation stage ... performed by a hierarchy of event analyzers ... to reduce the

number of security events, each event analyzer combines related security events

into a single security ticket. Event analyzers can also use the results of

vulnerability scans ... to prioritize detected security events" (10:62-67 and 11:1-

20). Thus the combination here provides an obvious disclosure of the reduction

of collected data for the benefit of allowing for more efficient analyzing of data.

Regarding <u>claim 12-14,</u> Teal is silent in disclosing a method wherein said

carrying out the additional test comprises reducing addresses in said first list and

said second list to reduced addresses, wherein the reduced addresses have a

smaller size and a constant predetermined relation with the addresses and at

least some of the addresses that differ are reduced to the same reduced

address, however Hrabik does provide such a disclosure (13:28-36 – "In addition

to the vulnerability and visibility scans, the master system 60 also verifies

services that directly affect the target network's connectivity but are typically out

of the network's control. This verification assessment ensures that company's

domain name was not "hijacked." The master security system conducts a

verification assessment of all information sources involved in network

connectivity verifying information from a root domain name servers all the way

through to a primary and a secondary web servers. The verification scan is

performed for the entire IP address group of the target company. For example,

when a target company has six IP addresses four of which are open and utilized

and two of which are blocked and not accessible, the verification scan

determines whether the blocked addresses remain unaccessible and whether the

open addresses remain accessible").

It would have been obvious for one of ordinary skill in the art, at the time of the

invention, to have been motivated to combine the disclosures of Teal with Hrabik

as both are directed towards protecting computer systems/networks from security breaches. Hrabik provides motivation for the combination in the recitation, "a fundamental weakness shared in common by current intrusion detection and response systems is their 'flat' or non-hierarchical implementation" (1:50-53) and further "after the events have been consolidated and classified, they enter the correlation stage … performed by a hierarchy of event analyzers … to reduce the number of security events, each event analyzer combines related security events into a single security ticket. Event analyzers can also use the results of vulnerability scans … to prioritize detected security events" (10:62-67 and 11:1-20). Thus the combination here provides an obvious disclosure of the reduction of collected data for the benefit of allowing for more efficient analyzing of data.

Regarding claim 15, Teal, discloses a method wherein said first and second monitoring comprises reducing information about said destinations, and storing at least one table about said data reduced information (4:23-25).

Regarding claim 16, Teal, discloses a method wherein said collection of data items further comprises a portion of a network header (4:16-27).

Regarding claim 17, Teal, discloses a method wherein said portion of a network header comprises a port number indicating a service requested by a network

packet (4:33-39 – "intrusion detection analysis engine 16 analyzes network data to look for specific patterns that indicate malicious activity on the network").

Regarding claim 18, Teal, discloses a method wherein said port number comprises a source port or a destination port (4:43-59)

Regarding claim 19, Teal, discloses a method wherein said data items comprise a first subset of a network packet including payload and header (4:16-27); and the method further comprises obtaining a second subset of the same network packet for subsequent analysis (4:33-39).

Regarding claim 20, Teal, discloses method further comprising forming a plurality of data items from each of a collection of network packets (4:16-27), each of said plurality of data items comprising a specified subset of the network packets (4:33-39).

Regarding claim 21, Teal, discloses a method further comprising forming a plurality of data items from each of a collection of network packets, each of said plurality of data items comprising a continuous portion of payload and information indicative of a port number indicating a service requested by the network packet (Rejected under the combined rationales as claims 11 and 20).

Regarding claim 22, Teal, discloses a method wherein said reducing said data
items and said determining frequently occurring sections comprises: taking a first
hash function of said data items first maintaining a first counter, with a plurality of
stages, and incrementing one of said stages based on an output of said first hash
function; taking a second hash function of said data items; and second
maintaining a second counter, with a plurality of stages, and incrementing one of
said stages of said second counter based on an output of said second hash
function (4:33-39 – "intrusion detection analysis engine 16 analyzes network data
to look for specific patterns that indicate malicious activity on the network").

Regarding claim 23, Teal, is silent in disclosing checking said one of said stages
of said first counter and said one of said stages of said second counter against a
threshold, and identifying a first reduced data item as associated with frequently
occuring content only when both said one of said stages of said first counter and
said one of said stages of said second counter are both above said threshold ,
however Hrabik does provide such a disclosure (11:50-54 – "Smart actions of the
provided security system are issued by event analyzers and can counteract a
threatening security event, for example, by increasing the level of detail recorded
on specific actions, IP addresses or users").

It would have been obvious for one of ordinary skill in the art, at the time of the
invention, to have been motivated to combine the disclosures of Teal with Hrabik

as both are directed towards protecting computer systems/networks from security

breaches. Hrabik provides motivation for the combination in the recitation, "a

fundamental weakness shared in common by current intrusion detection and

response systems is their 'flat' or non-hierarchical implementation" (1:50-53) and

further "after the events have been consolidated and classified, they enter the

correlation stage … performed by a hierarchy of event analyzers … to reduce the

number of security events, each event analyzer combines related security events

into a single security ticket. Event analyzers can also use the results of

vulnerability scans … to prioritize detected security events" (10:62-67 and 11:1-

20). Thus the combination here provides an obvious disclosure of the reduction

of collected data for the benefit of allowing for more efficient analyzing of data.

Regarding claim 24, Teal, discloses a method further comprising adding the first

reduced data item to a frequent content buffer table (Rejected under the same

rationale as claim 11).

Regarding claim 25, Teal, discloses a method further comprising taking at least a

third hash function of said data items, and incrementing a stage of at least a third

counter based on said third hash function, where said identifying said first

reduced data item as associated with frequently occurring content only when all

of said stages of each of said first, second and third counters are each above

said threshold (4:33-39 – "intrusion detection analysis engine 16 analyzes

network data to look for specific patterns that indicate malicious activity on the network").

Regarding claim 26, Teal, discloses a method further comprising obtaining said data items by taking a first part of messages, and subsequently obtaining a new data items by taking a second part of the messages (Rejected under the same rationale as claim 1).

Regarding claim 27, Teal, discloses a method wherein at least one of said hash functions comprises an incremental hash function (4:33-39 – "These patterns, known as signatures, are generally unique to each type of vulnerability of the network.").

Regarding claim 28, Teal, discloses a method wherein reducing said data items comprise hashing at least one of the source or destination, to form a collection of hash values, first determining a unique number of said hash values, and second determining a number of said one of source or destination addresses based on said first determining (Rejected under the same rationale as claim 8).

Regarding claim 29, Teal, discloses a method further comprising scaling the hash values prior to said second determining (Rejected under the same rationale as claim 8).

Regarding <u>claim 30</u>, <u>Teal</u>, discloses a method wherein said scaling comprises scaling by a first value during a first counting session, and scaling by a second value during a second measurement session (Rejected under the same rationale as claim 8).

Regarding <u>claim 31</u>, <u>Teal</u>, discloses a method wherein said detecting code comprises looking for a first valid opcode at a first location, based on said first valid opcode, determining a second location representing an offset to said first valid opcode, and looking for a second valid opcode at said second location (Rejected under the same rationale as claim 7).

Regarding <u>claim 32</u>, <u>Teal</u>, discloses a method further comprising establishing that a first section includes code when a predetermined number of valid opcodes are found at proper distances (Rejected under the same rationale as claim 7).

Regarding <u>claim 33</u>, <u>Teal</u>, discloses a method further comprising, determining a list of first computers that are susceptible to a specified attack, and monitoring only messages directed to said first computers for said specified attack (Rejected under the same rationale as claim 1).

Regarding <u>claim 34</u>, <u>Teal</u>, discloses a method where said monitoring comprises checking for a message that attempts to exploit a known vulnerability to which a computer is vulnerable, as said specified attack (Rejected under the same rationale as claim 1).

Regarding <u>claim 35</u>, <u>Teal</u>, discloses a method wherein said checking comprises checking for a field that is longer than a specified length (Rejected under the same rationale as claim 1).

Regarding <u>claim 69</u>, <u>Teal</u>, discloses a machine-implemented method for automatically identifying common content to use in identifying an intrusive network attack, comprising: monitoring network content on a network, and obtaining at least portions of the data on said network; data reducing said portions of the data using a data reduction function which reduces said portions of the data to reduced data portions in repeatable manner, such that each portion which has the same content is reduced to the same reduced data portion and at least some of the portions that differ are reduced to the same reduced data portion; analyzing said reduced data portions to find network content which repeats a specified number of times in order to establish said network content which repeats said specified number of times as frequent content; identifying address information of said frequent content, wherein the address information includes at least one of source information or destination information that

characterizes the respective of sources and/or destinations, of said frequent content, and determining if a number of sources and/or destinations of said frequent content is increasing; and identifying the frequent content as associated with the network attack, based on said identifying and determining (Rejected under the same rationale as claim 1).

Regarding claim 70, Teal, discloses a method as in claim 69, wherein said monitoring network content comprises obtaining both portions of the data on the network, and port numbers indicating a services requested by network packets (Rejected under the same rationale as claims 17 and 18).

Regarding claim 71, Teal, discloses a method as in claim 70, wherein said obtaining portions of the network data comprises: defining a window which samples a first portion of network data at a first time in accordance with a position of the window, and sliding said window to a second position at a second time which samples a second portion of said network data wherein said second position has a specified offset from the first portion (Rejected under the same rational as claim 1).

Regarding claim 72, Teal, discloses a method as in claim 71, wherein said data reduction function comprises a hash function (Rejected under the same rationale as claim 8).

Regarding <u>claim 73</u>, <u>Teal</u>, discloses a method as in claim 72, wherein said data reduction function comprises an incremental hash function (Rejected under the same rationale as claim 8).

Regarding <u>claim 74</u>, <u>Teal</u>, discloses a method as in claim 69, wherein data reducing said portions comprises using said data reduction function in a scalable configuration (Rejected under the same rationale as claim 8).

Regarding <u>claim 75</u>, <u>Teal</u>, discloses a method as in claim 69, wherein said identifying comprises second data reducing said address information using a data reduction function, and maintaining a table of data reduced address information (Rejected under the same rationale as claim 1).

Regarding <u>claim 76</u>, <u>Teal</u>, discloses a method as in claim 75, wherein said second data reducing comprises hashing said address information (Rejected under the same rationale as claim 8).

Regarding <u>claim 77</u>, <u>Teal</u>, discloses a method as in claim 69, further comprising testing contents of the frequent content to determine the presence of code in said frequent content (Rejected under the same rationale as claim 7).

Regarding claim 78, Teal, discloses a method as in claim 77, wherein said testing contents comprises identifying an opcode in said frequent content, determining a length of the opcode, and looking for another opcode at a location within said frequent content based on said length (Rejected under the same rationale as claim 7).

Regarding claim 79, Teal, discloses a method as in claim 69, further comprising monitoring for scanning of addresses (Rejected under the same rationale as claim 11).

Regarding claim 88. Teal discloses a machine-implemented method for automatically identifying common content to use in identifying an intrusive network attack, comprising: obtaining a collection of data items to be analyzed to identify the network attack; reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, wherein the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item; analyzing a plurality of said reduced data items to determine frequently occurring sections of message information indicative of a network attack; and carrying out an additional test on said frequently occurring sections of message information, comprising maintaining a first list of unassigned addresses,

wherein the unassigned addresses are maintained as reduced addresses that

have a smaller size and a constant predetermined relation with the unassigned

addresses and at least some of the unassigned addresses that differ are reduced

to the same reduced address, forming a second list of source addresses that

have sent to the unassigned addresses on said first list, wherein the source

addresses are maintained as reduced addresses that have a smaller size and a

constant predetermined relation with the source addresses and at least some of

the source addresses that differ are reduced to the same reduced address, and

comparing a current source of a frequently occurring section to said second list

(Rejected under the same rationale as claim 1 and 12).

Regarding claim 89. Teal discloses a machine-implemented method for

automatically identifying common content to use in identifying an intrusive

network attack, comprising: obtaining a collection of data items to be analyzed to

identify the network attack, wherein said data items comprise a first subset of a

network packet including payload and header; reducing said data items in said

collection to reduce said data collection to a reduced data collection of reduced

data items, wherein the reduced data items in the reduced data collection have a

smaller size and a constant predetermined relation with data items in the data

collection and at least some of the data items in the data collection that differ are

reduced to the same reduced data item; analyzing a plurality of said reduced

data items to detect common elements, said analyzing reviewing for common

content indicative of a network attack; and obtaining a second subset of the

same network packet for subsequent analysis (Rejected under the same

rationale as claim 1 and 12).

Conclusion

5.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to CHINWENDU C. OKORONKWO whose telephone

number is (571)272-2662. The examiner can normally be reached on MWF 2:30 - 6:00,

TR 9:00-3:30.

        If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone

number for the organization where this application or proceeding is assigned is 571-

273-8300.

        Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. C. O./
Examiner, Art Unit 2436

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436